DEPARTMENT OF THE
PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

Cyber Security Strategy Annual Report 2022/23

20 September 2023

Te Kāwanatanga o Aotearoa
New Zealand Government

Introduction

Cyber security remains a critical national security issue in New Zealand

1. Cyber security[1] is fundamental to the wellbeing of New Zealand and New Zealanders, supporting economic growth and prosperity, and protecting our national security. Digital technologies permeate almost every facet of our economy and society, offering significant opportunities for innovation, stronger productivity, and improved services. However, the benefits enabled by these technologies also come with new challenges, including increased exposure to cyber threats and attacks.

2. The recently released National Security Strategy highlights cyber security as one of 12 core issues that most directly impact New Zealand's national security interests[2]. Malicious cyber actors, including both state and non-state actors, present a persistent threat to all New Zealanders as well as New Zealand organisations, businesses and Government.

3. New Zealand is also facing an increasingly complex geostrategic environment in which cyber threats continue to evolve. Escalating geopolitical tensions can have significant impacts on the international cyber threat landscape, making it as important as ever for New Zealand to have a robust approach to cyber security.

The Cyber Security Strategy: enabling New Zealand to thrive online

4. New Zealand's Cyber Security Strategy 2019[3] (the Strategy) sets out the Government's commitment to keeping New Zealand safe, resilient, and prosperous online. It outlines areas where the Government is prioritising action, and how the Government will work with individuals, businesses, and communities to achieve its vision of a New Zealand that is confident and secure in the digital world.

5. The Strategy is underpinned by values that reflect New Zealand's unique place in the world, the Government's commitments to New Zealanders, and the need for citizens and industry to work together with the government to build a safe and trusted internet. These values are reflected in five priority areas for action to deliver the Strategy's overarching vision:

    a. Cyber security aware and active citizens

    b. Strong and capable cyber security workforce and ecosystem

    c. Internationally active

    d. Resilient and responsive New Zealand

    e. Proactively tackle cybercrime.

---

[1] "Cyber security" means protecting people and their computers, networks, programs, and data from unauthorised access, disruption, exploitation, or modification.

[2] https://www.dpmc.govt.nz/our-programmes/national-security/aotearoas-national-security-strategy

[3] https://www.dpmc.govt.nz/our-programmes/national-security/cyber-security-strategy

6. In 2019, an annual appropriation of $2 million was established on an ongoing basis to support implementation of the Strategy (referred to in this report as the Strategy implementation appropriation or the appropriation). This is in addition to existing appropriations for individual government agencies, which are crucial to lifting the cyber security and resilience of New Zealand.

7. The Strategy implementation appropriation is used to fund joint-agency projects to enhance national cyber security and lift cyber resilience at a system level. Projects and initiatives funded through the appropriation typically focus on priority areas that are not well addressed by existing government expenditure.

8. The Department of the Prime Minister and Cabinet (DPMC) is the administering agency for the appropriation. Individual projects may be proposed and project-managed by other agencies, and in some instances jointly managed between agencies. Governance for the appropriation is provided by the inter-agency Cyber Security Strategy Coordination Committee (CSSCC)[4].

Purpose of the Annual Report

9. The Strategy's responsible Minister is required to release a public annual report to update on progress made under each of the five priority areas. The responsible Minister is the Minister for the Digital Economy and Communications, to whom the Prime Minister has allocated responsibility for cyber security policy from the National Security and Intelligence portfolio.

10. The following section of the report outlines progress made under each priority area in FY 2022/23, including projects funded by the appropriation. It also includes overviews of some significant cyber security initiatives that, while not necessarily funded from the Strategy appropriation, are critical to enhancing cyber security and resilience in New Zealand. However, it does not include an exhaustive list of all cyber security-related activity undertaken by government agencies.

[4] Agencies regularly attending the committee include: DPMC, National Security Group (Chair); DPMC, National Cyber Policy Office (NCPO); CERT NZ; Department of Internal Affairs (DIA); Government Communications Security Bureau (GCSB), National Cyber Security Centre (NCSC); Ministry of Defence (MoD); Ministry of Foreign Affairs and Trade (MFAT); Ministry of Justice (MoJ); New Zealand Defence Force (NZDF); New Zealand Police (NZP). Other agencies attend on occasion, as required.

Cyber Security Strategy implementation in 2022/23

Summary

11. Over the past year, the Government has overseen a significant programme of work across the Strategy's five priority areas, both through the Strategy implementation appropriation and agencies' individual work programmes.

12. These initiatives delivered a range of benefits for New Zealand, by:

    a. supporting increased engagement and involvement by the public in cyber security issues, by improving accessibility to cyber resources for diverse communities, launching educational programmes for school-aged children, and working with Māori subject matter experts to design a bespoke model for Māori involvement in New Zealand's approach to cybercrime;

    b. addressing information gaps by commissioning research projects to support evidence-based policy responses to current and emerging trends, such the impact of emerging and disruptive technologies on law enforcement in New Zealand;

    c. streamlining and strengthening operational structures and information flows within and between agencies, by working to consolidate cyber incident reporting functions (currently underway), broadening secondment opportunities to share and build limited cyber expertise across agencies, and building a business case to establish a permanent cyber exercise capability;

    d. representing and promoting New Zealand's interests internationally, including information-sharing on threats, trends and policy responses with close partners, participating in UN processes and negotiations on cyber security and cybercrime, and engaging in other regional, multilateral, and multistakeholder forums on cyber security;

    e. supporting our Pacific partners to build and strengthen their own cyber capabilities, as well as participate in international forums to promote their perspectives on key issues.

Priority area 1: Cyber security aware and active citizens

13. This priority area aims to build a culture in which New Zealanders can operate securely online and know what to do if something goes wrong. This includes initiatives targeted at building general skills and awareness of cyber issues across New Zealand.

14. Over the past year, CERT NZ made further progress on two existing initiatives under this priority area:

    a. **Translation of CERT NZ resources into Māori, New Zealand Sign Language, and other languages**: Building on the successful translation of CERT NZ guidance into 13 languages (completed in FY 2021/22), this phase of the project involved turning these resources into video format to further increase accessibility. The videos are being completed and will be distributed in FY 2023/24.

    b. **Cyber security market research on behaviours to inform awareness campaigns**: CERT NZ commissioned research on New Zealanders' motivations and barriers to protecting themselves online, to support the development of more successful cyber awareness campaigns. This resulted in the publication of a 'Cyber Change' booklet[5], which ties research with behavioural science insights to help both government and industry organisations develop successful cyber security interventions.

15. In addition, both CERT NZ and the NCSC regularly publish cyber security guidance and advice for New Zealand individuals and businesses. This includes advisories on dealing with specific ransomware tools such as LockBit[6], alerts about scams targeting New Zealanders such as a credit card scam campaign[7], and best practice principles for secure-by-design and secure-by-default software for manufacturers and customer organisations.[8]

[5] https://www.cert.govt.nz/assets/resources/cert-nz-cyber-change-behavioural-insights-2022-online-version.pdf

[6] https://www.ncsc.govt.nz/news/joint-advisory-lockbit/

[7] https://www.cert.govt.nz/individuals/alerts/credit-card-scam-text-message-campaign-targets-new-zealanders/

[8] https://www.ncsc.govt.nz/news/security-by-design/

Priority area 2: Strong and capable cyber security workforce and ecosystem

16. The purpose of this priority area is to ensure that New Zealand can rely on a strong cyber security workforce and sector, capable of preventing and responding to a range of cyber threats. This includes efforts targeted at building baseline skills, increasing the profile of cyber careers, and developing a diverse domestic cyber talent pipeline.

17. Three initiatives were funded by the Strategy implementation appropriation in FY 2022/23:

    a. **Cyber Skills Aotearoa**: This programme, co-funded by government, provides activities and resources to teachers and students to develop their cyber security capabilities. On 8 November 2022, Ministers launched the programme at an event hosted by Naenae College, in partnership with programme developer Grok Academy, Tātai Aho Rau CORE Education, CSSCC agencies, and industry representatives. Full details about the programme, including available and upcoming courses and competitions, can be found on the Grok Academy website[9].

    b. **Cyber security workforce research project**: DPMC commissioned research to scope the New Zealand cyber security workforce across the public and private sectors, to include roles, size, demographics, and key skills gaps. The supplier has completed the main report, which included several instructive insights that helped to shape policy work on this topic. The supplier has also been contracted to produce three annual monitoring reports in the coming years to track progress on this issue.

    c. **Manu Kurutao: Digital training pilot for Māori**: This is the second phase of a project developed by the organisation Tokona Te Raki, which aims to develop a training pathway for rangatahi Māori in cyber security. This phase, which is currently underway, involves a 24-week programme on cyber security with both course-based activity and work placements for programme participants.

18. In addition to Strategy-funded initiatives, in May 2023 MBIE published the Digital Technologies Industry Transformation Plan (ITP), which is a long-term vehicle for partnership between industry and government in the digital technologies sector. The ITP includes a focus area ‘enhancing the digital technologies skills and talent pipeline’, as a critical enabler for the sector and the wider tech workforce. This is a key mechanism for the delivery of initiatives to grow the cyber security workforce, as the skills challenges and opportunities faced by the cyber security sector share several commonalities with those experienced by the digital technologies sector more broadly.

[9] https://groklearning.com/cyber-nz/

Priority area 3: Internationally active

19. This priority area is about advancing and protecting New Zealand's cyber interests through our international activity. This includes responding to unacceptable behaviour online, cooperating with international partners to share information and prevent and deter malicious activity that threatens peace and security in cyberspace, and supporting cyber capacity building in the Pacific and beyond.

20. Two initiatives funded by the Strategy implementation appropriation were progressed in FY 2022/23:

    a. **Women in International Security and Cyberspace Fellowship (WIC): international workshop contribution**: The New Zealand Government partnered with the NGO Diplo in 2022 to offer their 'cybersecurity diplomacy' online course to WIC fellows over six weeks in September and October 2022. Diplo received overwhelmingly positive feedback on the course, with 100% of respondents reporting that the course either met or exceeded expectations.

    b. **Global Forum for Cyber Expertise (GFCE) contribution**: The GFCE invited New Zealand to take a seat on the Steering Committee for the Global Conference on Cyber Capacity building, which was originally scheduled to take place in Washington DC in May 2023. The CSSCC endorsed a proposal to support a Pacific partner to take up the seat with our support, aligning with New Zealand's Pacific Resilience approach and broadening the perspectives on the Steering Committee. The conference itself has since been postponed to November 2023.

21. In addition to the initiatives above, there is a significant programme of international engagement with bilateral partners and in multilateral and multistakeholder forums, the funding for which generally comes from agency baselines rather than Strategy implementation funding. This includes:

    a. **Cyber Security Support to the Pacific Programme (CSSP)**: This programme serves as a mechanism for New Zealand agencies provide cyber capacity building and supports identified cyber needs in the region. Since its establishment in 2019, the CSSP has:

        i. supported the establishment of a Samoan CERT;

        ii. supported the development of Tokelau's Cyber Rules;

        iii. funded New Zealand Police's contribution to Cyber Safety Pasifika;

        iv. enabled CERT NZ to provide peer support to Pacific governments.

    b. **Engagement in multilateral and multistakeholder forums** – Over the past year, government agencies have continued to engage extensively in multilateral and multistakeholder forums to promote New Zealand's cyber security interests. This includes:

        i. active membership in the US-led International Counter Ransomware Initiative (CRI) and its operational and policy sub-groups, which aims to build resilience to ransomware attacks through developing effective policies and responses in collaboration with other participating states;

ii. attending (virtually and in-person) the United Nations (UN) International Telecommunications Union (ITU) Plenipotentiary Conference in Bucharest, where MBIE and DPMC officials participated in negotiations to promote the development and adoption of ICT standards in line with New Zealand's interests;

iii. participating in and contributing to the UN cybercrime convention negotiations, advocating for a convention that should have a sharp focus on core cybercrime issues and complement existing UN conventions rather than conflict with them[10];

iv. participating in the UN Open-Ended Working Group (OEWG) on 'security of and in the use of information and communications technologies', which aims to further develop the rules, norms and principles of responsible state behaviour in cyberspace;

v. CERT NZ's work with likeminded partners to develop joint international guidance[11] urging software manufacturers to take the steps necessary to ship products that are secure-by-design and by-default;

vi. supporting the Prime Minister's attendance at the March 2023 Summit for Democracy, which included signing on to the Joint Declaration calling for the promotion of the framework for responsible state behaviour in cyberspace, and for an open, free, accessible, and secure Internet (amongst a range of other issues).

c. **Joint cyber security advisories** – The NCSC joined like-minded international partners in calling out malicious cyber activity sponsored by nation states through the publication of cyber security advisories. These advisories highlight the malicious activity undertaken and provide extensive technical information and mitigations for the defence of networks. Recent examples include the advisories regarding the Russian 'Snake' malware variant[12] and activity associated with a People's Republic of China (PRC) state-sponsored cyber actor 'Living off the Land'[13].

d. **International events and cooperation** – In October 2022, the Minister for the Digital Economy and Communications attended Singapore International Cyber Week, supported by officials from DPMC and CERT NZ. Organised by the Cyber Security Agency of Singapore, Singapore International Cyber Week brings together global policy makers, industry leaders and academia to exchange best practices and strengthen international cooperation on cyber security topics. Attendance at this event strengthened New Zealand's relationships with key partners, promoting New Zealand's values and interests at a major international cyber security forum.

---

[10] New Zealand's full submission to the first session of negotiations can be found here: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/New_Zealand_National_Submission_-_AHC.pdf

[11] https://www.cert.govt.nz/individuals/news-and-events/international-guidance-princles-and-approaches-to-secure-by-design-and-by-default/

[12] https://www.ncsc.govt.nz/news/joint-advisory-russian-intelligence-snake-malware/

[13] https://www.ncsc.govt.nz/news/prc-cyber-actor-targeting-us-critical-infrastructure-guidance-to-assist-detection/

e. **Bilateral and multilateral engagement with close partners** – New Zealand frequently engages with close international partners on cyber security policy and operational issues. This included hosting the Five Country Ministerial (FCM) meeting in Wellington in June 2023, which involved bilateral and group discussions on key cyber security issues, among other areas of focus. Key outcomes of the FCM were highlighted in the Five Country Ministerial Communiqué[14].

Priority area 4: Resilient and responsive New Zealand

22. This priority area focuses on enhancing New Zealand's ability to resist cyber threats, and ensuring we have the tools and know-how to protect ourselves.

23. Four initiatives were funded by the Strategy implementation appropriation in this priority area in FY 2022/23:

    a. **National cyber security exercise capability project**: NCSC is developing a business case for an ongoing national cyber security exercise capability to test government and industry responses to major cyber incidents.

    b. **Horizon scanning research on existing and emerging technologies**: DPMC commissioned research on emerging and disruptive technologies and their impact on public safety over the next 3-5 years. The final report provided comprehensive and valuable insights on three technologies, as well as the approach taken by different government agencies to analyse the benefits and risks of these technologies. The CSSCC will consider next steps on the report's recommendations in early FY 2023/24.

    c. **National-level strategic cyber security risk assessment**: DPMC commissioned a report on the key cyber security risks facing New Zealand, to enhance government officials' and decision makers' understanding of the cyber risk landscape. The final report is expected in FY 2023/24.

    d. **Completing the work of the Cyber Security Advisory Committee** (CSAC): CSAC advice continued to provide input to advice considered by Cabinet regarding cyber resilience. In August 2022, CSAC provided its final advice to the Minister for the Digital Economy and Communications on the potential form and function of a public-facing 'single front door' for government cyber security advice.

[14] https://www.beehive.govt.nz/release/five-country-ministerial-communique-1

24. In addition to the Strategy-funded initiatives above, CERT NZ carries out ongoing work to respond to cyber incidents and help educate and inform the public about ways to prevent cyber incidents. CERT NZ also has several ongoing workstreams that support cyber security resilience, including:

    a. **Single reporting platform**: CERT NZ is developing a technology solution to make it easier for individuals and organisations to report cyber incidents, and to coordinate responses across all of the responsible government agencies.

    b. **Get Cyber Smart programme uplift**: This programme aims to increase awareness of CERT NZ's cyber security advice and reach a greater number of individuals and small-to-medium businesses, in order to improve security practices.

    c. **Cyber navigators' service**: This service leverages third-party business networks to provide specific cyber security advice to businesses in their communities.

    d. **Victim remediation pilot**: This pilot offers a service to assist victims of cyber incidents to recover and become more resilient to future incidents.

    e. **Denial of service public/private partnership**: This partnership aims to investigate and test innovative solutions to reduce the risk of future denial of service attacks and explore the opportunity to make this protection more cost effective for all organisations.

    f. **Cyber resilience measurement framework**: CERT NZ is developing specific metrics about cyber resilience so that the government can consistently measure overall cyber resilience and target initiatives appropriately.

25. Other agencies have also progressed initiatives independently from the Strategy implementation appropriation. Two significant projects include:

    a. **Lifting the resilience of New Zealand's critical infrastructure**: DPMC is leading a work programme that aims to lift the resilience of New Zealand's critical infrastructure, including to cyber threats. This work will include extending New Zealand's regulatory approach to cover a wide range of risks, including cyber risks, and impose clear, consistent standards to protect critical assets against risks to information and operational technology. DPMC undertook public consultation from 13 June to 8 August 2023, engaging critical infrastructure owners and operators, local government, and the public on how we can collectively lift our resilience. A second round of consultation on specific resilience policy options is expected in the first half of 2024.

    b. **Operational improvements to the cyber incident reporting and response system**: In addition to CERT NZ's work on developing a single reporting platform for incidents, this project aims to make operational improvements to how Government agencies manage and respond to these incidents once reported.

Priority area 5: Proactively tackle cybercrime

26. This priority area focuses on strengthening New Zealand's ability to proactively and collaboratively prevent, investigate, deter and respond to cybercrime, cyber-enabled crime and terrorist use of the Internet.

27. Three initiatives were funded by the Strategy implementation appropriation in FY 2022/23 under this priority area:

    a. **Budapest Convention consultation**: DPMC and the Ministry of Justice undertook targeted consultation to develop a bespoke mechanism for ongoing Māori involvement in New Zealand's implementation of the Budapest Convention on Cybercrime.

    b. **Cybercrime risk landscape assessment**: NZ Police has commissioned research to assess significant financially motivated transnational organised cybercrime threats to New Zealand, develop a national picture of cybercrime, and produce an initial methodology for ongoing assessments of the range, scale, and nature of cyber harms. NZ Police expects that the final report will be submitted in FY 2023/24.

    c. **NZ Police / NCSC staff secondments**: In 2022 NZ Police directly funded the secondment of an analyst into the NCSC, which helped to expand NZ Police's cybercrime expertise. Building on the success of this initial secondment, the CSSCC has endorsed a proposal to fund two new analytical positions (one in each agency) focused on cybercrime.

28. Other work programmes underway to address this priority area include:

    a. **Encryption Working Group (EWG)**: The CSSCC established a cross-agency working group to analyse the impact of applications using end-to-end encryption (E2EE) on law enforcement investigations, and to explore whether any policy changes are merited. In May 2023, the EWG produced an interim report with four recommendations. Agencies are currently working through what resources would be required to progress each recommendation and will report back to the CSSCC in early FY 2023/24 on proposed next steps.

    b. **Accession to the Budapest Convention on Cybercrime**: In December 2020, Cabinet agreed to accede to the Budapest Convention on Cybercrime. The Bill to enable New Zealand's accession to the Budapest Convention is due to be introduced to Parliament after the 2023 general election.

    c. **UN Cybercrime Convention**[15]: The fourth and fifth rounds of negotiations of the UN Cybercrime Convention took place in 2023. New Zealand Government officials continued to advocate that the Convention should have a sharp focus on core cybercrime issues and complement existing UN conventions rather than conflict with them.[16] The sixth and final session of negotiations takes place in August 2023.

---

[15] Known as the 'Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes'.

[16] New Zealand's full submission to the first session of negotiations can be found here: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/New_Zealand_National_Submission_-_AHC.pdf

d. **Ransomware guidance**: In April 2023, the government issued guidance on cyber ransom payments[17]. This reflects that Cabinet has agreed that government agencies do not pay cyber ransoms. It also sets out that the government strongly discourages the payment of ransoms to cybercriminals, and urges all victims to report any cyber ransom incidents to the relevant agencies, regardless of whether a ransom is paid.

e. **Phishing disruption service**: CERT NZ's phishing disruption service shares high-confidence and actionable information about phishing incidents that specifically affect New Zealanders and/or misrepresent New Zealand brands. It is intended to help reduce the impacts of phishing on New Zealanders and is available to all New Zealand organisations. CERT NZ is continuing to develop this service to increase uptake and submissions to the service from the private and public sectors.

Administrative costs

29. Since FY 2021/22, the Strategy implementation appropriation has funded the salaries of up to 5.8 FTEs to better deliver the Strategy, including the Cyber Coordinator, a Programme Advisor to support the CSSCC and appropriation expenditure, and Principal and Senior Advisors in NCPO working on cross-sector policy work. These FTEs have enabled the delivery of high priority workstreams, including the extensive policy work and Māori engagement to support New Zealand's accession to the Budapest Convention, as well as work on cyber security workforce development, and industry growth.

30. In addition, a contribution from the Strategy implementation appropriation to the Christchurch Call Unit has supported 4.25 FTEs (MFAT also provides FTEs to the unit). This gives effect to a range of values and priorities in the Strategy, including protection from online harms, Internet governance and partnerships with the private sector.

[17] https://www.dpmc.govt.nz/our-programmes/national-security/cyber-security-strategy/cyber-ransom-advice